Route Educational and Social Science Journal ISSN: 2148-5518

Volume 5(7), May 2018

Article History		
Received/Geliş	Accepted/ Kabul	Available Online / Yayınlanma
2 /5/2018	11 /5/2018	15 /5/2018

الاستراتيجية الأممية لحماية الأمن الإلكتروني

د .بوحفص جلاب نعناعة

جامعة البليدة – 2–

الملخص

يشهد العالم تطوراً مذهلاً في مجال المخاطر الأمنية ، وقد تزامن مع تطور مراحل النضج التكنولوجي ، بالانتقال من مرحلة النمو السريع الى مرحلة الاستخدام الكثيف ،فاصبح للفضاء الالكتروني دورا في حركة التفاعلات و التحولات البنيوية و كمجال جديد في العلاقات الدولية، حيث بدأ ينتقل تأثيره من تغييرات هيكلية وتحتية الى تغييرات كيفية مؤثرة في النظام الدولي.

انعكس دخول المجال الإلكتروني، ضمن محددات وابعاد القوة الدولية من حيث طبيعتها وأنماط استخدامها وطبيعة الفاعلين فيها ،على قدرات الدول وعلاقاتها الخارجية، فأضفى خصائص جديدة للقوة، باستخدام أسلحة تكنولوجيا الاتصال والمعلومات ضد المنشآت المدنية والعسكرية وأنظمة الدول والمؤسسات السياسية وإفسادها، فأضحى سبيلاً لمحاولة السيطرة الواسعة على المؤسسات الحيوية للدول الأخرى، و تهديدا مباشرا لأمنها القومي.

تعالج الورقة مسألة الامن الإلكتروني، كأحد أهم المواضيع التي تشكل أساساً جوهرياً لاستراتيجيات الدول والمنظمات الدولية العالمية والإقليمية، الحكومية وغير الحكومية، لمواجهة مختلف الجوانب التي تهدد استقرار الفضاء الرقمي و السلم والأمن الدولي فتحاول الإجابة عن الاشكالية التالية: الى أي مدى استطاعت قواعد القانون الدولي من ضبط أنشطة الدول في الفضاء الإلكتروني ودعم الأمن الإلكتروني.

لتحقيق هدف هذه الدراسة قامت الباحثة بمعالجة هذا الموضوع من خلال بيان المفاهيم الخاصة بالأمن الإلكتروني كمبحث أول والتعرف على إشكاليات المجتمع الدولي في التعامل مع الأسلحة الإلكترونية في المبحث الثاني و اخيرا مضمون الرؤية الشاملة لمستقبل التعاون الدولي المتعلق بالأمن الإلكتروني في المبحث الثالث و ختمت الدراسة بأهم النتائج و التوصيات.

الكلمات المفتاحية :الامن الالكتروني ،المخاطر الامنية، أسلحة تكنولوجيا الاتصال والمعلومات، القوة الدولية، النظام الدولي

الاستراتيجية الأممية لحماية الأمن الإلكتروني

د .بوحفص جلاب نعناعة

The UN Strategy for the Protection of Electronic Security

Dr.. Bouhafs Djellab Nanaa

University of Blida 2

Abstract

The world is witnessing a remarkable development in the field of security risks. It has coincided with the development of the stages of technological maturity, moving from the stage of rapid growth to the intensive use stage. Electronic space has a role in the movement of interactions and structural transformations , and as a new field in international relations. Structural and subversive to how influential changes in the international system.

The entry of the electronic domain, within the limits of the international power in terms of its nature, patterns of use and the nature of its actors, has reflected on the capabilities of States and their external relations. adding new characteristics to the force, using ICT weapons against civil and military installations and the systems of states and political institutions.

The paper tackles the issue of electronic security as one of the most important topics that constitutes a fundamental basis for the strategies of international and regional governmental and non-governmental organizations and states to confront various aspects that threaten the stability of digital space , peace and international security. From controlling the activities of States in cyberspace and supporting electronic security.

In order to achieve the objective of this study, the researcher addressed this issue by presenting the concepts of electronic security in the first vital institutions of other States, and a direct threat to their national security .part of the study and identifying the problems of the international community in dealing with electronic weapons in the second section. finally the content of the comprehensive vision for the future of international cooperation on electronic security in the third section and followed by recommendations.

Key words: electronic security, security risks, communications and information technology weapons, international force, international system

الاستراتيجية الأممية لحماية الأمن الإلكتروني

د .بوحفص جلاب نعناعة

مــقدمة

لقد أصبح الأمن القومي مهددا من طرف العولمة و تكنولوجيا الاتصال الحديثة ،لذا يرتكز الأمن الإلكتروني على تعزيز الحماية للحد من مخاطر التكنولوجيا الرقمية بسبب استخدامها المتزايد للأغراض غير القانونية، بضمان سرية و سلامة المعلومات و البيانات من كل الهجمات الإلكترونية ، كما يفرض أليات غير تقليدية لمواجهة مختلف الأخطار غير المرئية و العابرة للحدود و التي تقوم على اختراق البنى التحتية للاتصالات و قواعد البيانات والمعلومات للدول .

أصبحت الأنترنت تستعمل لتفكيك المركز القانوني والتنظيمي والسيادي للدول و إعادة هندسة اشكال جديدة للسيطرة و الهيمنة، لذا يعد الأمن الإلكتروني من أهم المواضيع التي تشكل أساسا لاستراتيجيات الدول والمنظمات الدولية العالمية والإقليمية، الحكومية وغير الحكومية، لمواجهة مختلف المشاكل التي تهدد استقرار الفضاء الرقمي، والذي سينعكس سلبا على السلم والأمن الدوليين.

تحول الفضاء الإلكتروني إلى ساحة للتفاعلات الدولية، فبرزت العديد من الأنماط التوظيفية له، على صعيد الاستخدامات ذات الطبيعة المدنية أو العسكرية، الأمر الذي جعله مجالا للصراعات المختلفة للفاعلين من الدول أو غير الدول من أجل حيازة أكبر قدر من النفوذ والتأثير السيبراني.

تناقش هذه الورقة مسألة الأمن الإلكتروني و الأطر المرتبطة والمفسرة له باعتباره من أهم التحديات التي تواجه المنظمات الدولية و الصكوك الدولية و المحافل العالمية بسبب ارتباطه بالعديد من المخاطر الأمنية و الجرائم المنظمة كالقرصنة الإلكترونية التي تهدد الفضاء الالكتروني .

المشكلة البحثية

رغم النجاح الباهر للأنترنت إلا ان هذا التقدم في الوقت ذاته، جعل الدول عرضة لهجمات إلكترونية على نحو يثير القلق و منه أهمية الأمن الإلكتروني في النظام الدولي بعد تزايد الاعتماد على التكنولوجيا.

ساعد الفضاء الإلكتروني على انتهاء احتكار القوة بالمعنى التقليدي والمتمثلة في القوة الصلبة، وظهور نوع جديد من القوة هي القوة الالكترونية أو الافتراضية، التي أصبحت في متناول كل من يمتلك المعرفة التكنولوجية و القدرة على استخدامها في ظل المتغيرات والتحولات الاقليمية والدولية لتحقيق أهدافه، ولو بشكل غير سلمي .

و منه سنحاول من خلال هذه الدراسة الإجابة على: الاشكالية الرئيسية: **ما هي ابعاد الاستراتيجيات الدولية لحماية الامن الالكتروني؟**

و الاسئلة الفرعية : **–ما هو مفهوم الامن الإلكتروني و ما قاربه من مفاهيم مستحدثة في اطار المفهوم العام للفضاء الإلكتروني؟**

–ماهي مخاطر الفضاء الالكتروني على سيادة الدول؟

–ما هي أبعاد الاستراتيجيات على الساحة الدولية لمواجهة مخاطر الحروب الالكترونية و تحقيق الامن الالكتروني؟ و كيف يمكن تحقيق الأمن الالكتروني في ظل التحديات الخطيرة و الجديدة التي تواجه الدول من منظور استراتيجي في إطار مساعي المنظمات الدولية و الصكوك الدولية ؟

أهمية الدراسة:

1-الأهمية العلمية

ليس للثورة التكنولوجية تأثيرات ايجابية فقط ولكن لها اثار سلبية ومن هنا تأتى الأهمية العلمية للدراسة حيث انها توضح مضمون الاستراتيجيات المعتمدة على الساحة الدولية، لضمان الأمن الإلكتروني وتتناول القضايا المتعلقة بهذا المفهوم وتوضح خصائص واشكال واليات الامن الإلكتروني، و علاقة ذلك بتغيير مفهوم القوة في النظام الدولي وظهور القوة الالكترونية وانتهاء عصر احتكار القوة.

كما تأتي أهمية الدراسة من جانب تأثير الفضاء الإلكتروني على العلاقات الدولية و ان فهم السياسة الدولية، عبر مرحلة تاريخية معينة، يتطلب التعرف علي ماهية العناصر، وكيفية تفاعلها عبر أدوات تكنولوجيا الاتصال، والمعلومات التي ساعدت في قيادة التغيير.

أصبح توفر الأمن الالكتروني من مكونات السياق الدولي، ومحددا لطبيعة وخصائص وأطراف العلاقات الدولية، في إطار بزوغ ظاهرة الفضاء الإلكتروني، كمجال جديد في العلاقات الدولية، وما فرضه من تحديات تطبيقية، وأخري نظرية تتعلق من ناحية بتصاعد دور الفضاء الإلكتروني في حركة العلاقات الدولية، ومن جهة أخرى بمدى تأثيره في القدرة التفسيرية والنظرية للعلاقات الدولية و بنية الأمن العالمي.

2-الاهمية العملية

بعد عرض الدراسة للمفاهيم النظرية المتعلقة بمخاطر الفضاء الإلكتروني، تبحث في سبل تنسيق الدول لجهودها من أجل التعامل معها بجدية ،لان الهجمات الالكترونية تستهدف النظم و البرامج للبنية التحتية الحيوية للدول فهي تعتبر تهديدات جدية ،خطيرة و محتملة الحدوث تفرض استراتيجيات دولية لحماية الامن الالكتروني و مكتسبات المجتمع الدولي و مقومات الحياة.

الدراسات السابقة:

هناك العديد من الدراسات التي تناولت الهجمات الالكترونية و حروب الشبكات والاتصالات والحروب التكنولوجية و تأثيراتها على الامن الالكتروني على المستوى الدولي .

تم التركيز على الدراسات التي بحثت في اثر الفضاء الإلكتروني على تغير القوة في العلاقات الدولية والنظام الدولي و استراتيجيات حمايته منها:

1- عادل عبدالصادق الجخة،(2014)، اثر الفضاء الإلكتروني في تغير طبيعة العلاقات الدولية: دراسة في النظرية والتطبيق،(دكتوراه)، جامعة القاهرة، كلية الاقتصاد والعلوم السياسية.

2-ايهاب عبدالحميد خليفه عبدالعال،(2015)، استخدام القوة الالكترونية في ادارة التفاعلات الدولية: الولايات المتحدة نموذجاً 2001- 2012،(ماجيستير)، جامعة القاهرة، كلية الاقتصاد والعلوم السياسية

3- نوران شفيق علي،(2014)، الفضاء الإلكتروني وأنماط التفاعلات الدولية: دراسة في أبعاد الأمن الإلكتروني،(ماجيستير)، جامعة القاهرة، كلية الاقتصاد والعلوم السياسية.

4-حامد ابن قنيفذ ونس الشمري ،(2015)، رؤية استراتيجية لحماية الفضاء الالكتروني للملكة العربية السعودية (ماجيستير)، جامعة نايف العربية للعلوم الامنية كلية العلوم الاستراتيجية

منهجية الدراسة:

استخدمت الباحثة المنهج الوصفي التحليلي بالإضافة الى المنهج الاستقرائي الاستنباطي من اجل الوصول الى اكبر قدر من المصداقية كما تعتمد الدراسة على تحليل الآراء الفقهية ومناقشتها ، ولم تغفل الدراسة الرجوع إلى المواقع الإلكترونية المتخصصة التي تُعد من المصادر التي تستحق الاهتمام. **وقد جرى تقسيم هذه الدراسة على النحو الآتي:**

المبحث الأول: المفاهيم الخاصة بالأمن الإلكتروني

المبحث الثاني :إشكاليات المجتمع الدولي في التعامل مع الأسلحة الإلكترونية

المبحث الثالث: مضمون الرؤية الشاملة لمستقبل التعاون الدولي المتعلق بالأمن الإلكتروني

المبحث الأول

المفاهيم الخاصة بالأمن الإلكتروني

دخل الامن الإلكتروني ضمن المحددات الجديدة للقوة وأبعادها من حيث طبيعتها وأنماط استخدامها في الحروب بل وايضا طبيعة الفاعلين فيها وهو ما كان له انعكاس على قدرات الدول وعلاقاتها الخارجية.

اولا : مفهوم الأمن الإلكتروني وطبيعة تداخلاته

برزت مفاهيم خاصة لها علاقة بالأمن الإلكتروني ،خصائصه، صوره، وأبعاده. كمفاهيم حديثة أنتجتها التكنولوجيا منها:

1-الفضاء الإلكتروني:

الفضاء أو المحتوى والبديل الكوني الذى يمكن الناس من المشاركة فيه، ويصفه" وليام جيبسون" بأنه العالم الرقمي وهو عباره عن شبكات الكمبيوتر والاتصالات الإلكترونية خيالية تحتوى على كم هائل من المعلومات التي يمكن الحصول عليها لتحقيق الثروة والسلطة، حيث تقترب العلاقة بين العالم المادي والعالم الواقعي .

الفضاء الإلكتروني شأنه شأن كلمة الفضاء التقليدية يتألف من أربعة مكونات رئيسية هي المكان والمسافة والحجم والمسار ويتميز الفضاء الإلكتروني بغياب الحدود الجغرافية[1]

2-القوة السيبرانية:

يلعب الفضاء الإلكتروني دورا أساسيا في تعظيم القوة، أو الاستحواذ على عناصرها الأساسية في العلاقات الدولية، و في تغيير مفهوم القوة الوطنية للدولة، فبات بالإمكان تعريفها بأنها" مجموعة الوسائل، والطاقات، والإمكانيات المادية وغير المادية، المنظورة وغير المنظورة التي بحوزة الدولة، ويستخدمها صانع القرار في فعل مؤثر يحقق مصالح الدولة، وتؤثر في سلوك الوحدات السياسية الأخرى[2]

في غمار هذا التحول، برزت "القوة السيبرانية"، إذ عرفها جوزيف ناي بأنها "مجموعة الموارد المتعلقة بالتحكم في والسيطرة على أجهزة الحاسبات والمعلومات، والشبكات الإلكترونية، والبنية التحتية المعلوماتية، والمهارات البشرية المدربة للتعامل مع هذه الوسائل ."ترتكز عناصر

1-رؤية استراتيجية لحماية الفضاء الالكتروني للملكة العربية السعودية ، ابن قنيفذ ونس الشمري(2015) جامعة نايف العربية للعلوم الامنية كلية العلوم الاستراتيجية ، ص 8

2- المنازعات الدولية: مقدمة للنظرية والتاريخ ،جوزيف س. ناي الابن، ، ترجمة: أحمد أمين الجمل، ومجدي كامل ،القاهرة: الجمعية المصرية لنشر المعرفة والثقافة العالمية، ص 82

تلك القوة على وجود نظام متماسك يعظم القوة المتحصلة من التناغم بين القدرات التكنولوجية، والاقتصادية، العسكرية، وإرادة الدولة، وغيرها بما يسهم في دعم إمكانات الدول على ممارسة الإكراه، أو الإقناع، أو ممارسة التأثير السياسي في أعمال الدول الأخرى بغرض الوصول للأهداف الوطنية، من خلال قدرات التحكم، والسيطرة على الفضاء الإلكتروني.

أعطت القوة السيبرانية دفعا رئيسيا في اتجاهين الاول في تدعيم القوة الناعمة للدول، حيث بات الفضاء الإلكتروني مسرحا لشن هجمات تخريبية ترتبط بنشر المعلومات المضللة، والحرب النفسية، والتأثير في توجهات الرأي العام، والنشاط السري والاستخباراتي والثاني يتعلق بتبني الدول الزيادة في الإنفاق في اطار سياسات الدفاع الإلكتروني، وتوفير الامن الالكتروني من خطر التهديدات، وبناء مؤسسات وطنية للحماية الإلكترونية.

إن القوة الالكترونية فرضت تحديات على الأطراف الدولية وخاصة الكبرى ،التي كانت تحتكر مصادر القوة مثل الولايات المتحدة الأمريكية، فانتقلت القوة وانتشرت بين أطراف متعددة سواء كانت دول أو غير دول.

3-الحرب الإلكترونية

هي كل عمل عدائي في الفضاء الإلكتروني بضخامة أو يعادل تأثير العنف البدني الجسيم ولقد أصبح التفوق في مجال الفضاء الإلكتروني عنصرا حيويا في تنفيذ عمليات ذات فاعلية ،باعتماد القدرة القتالية في الفضاء الإلكتروني ،على نظم التحكم والسيطرة[3]

ليس هناك إجماع واسع على تعريف محدد ودقيق لمفهوم الحرب الإلكترونية وعلى الرغم من ذلك، فقد اجتهد عدد من الخبراء في تقديم تعريف يحيط بهذا المفهوم، فعرف كل من "ريتشارك كلارك" و"روبرت كناكي" الحرب إلكترونية على أنها "أعمال تقوم بها دولة تحاول من خلالها اختراق أجهزة الكمبيوتر والشبكات التابعة لدولة أخرى بهدف تحقيق أضرار بالغة أو تعطيلها[4].

يتعلق مضمون الحرب الإلكترونية بالتطبيقات العسكرية للفضاء الإلكتروني ، حيث تعني قيام دولة أو فواعل من غير الدول بشن هجوم إلكتروني في إطار متبادل، أو من قبل طرف واحد، ورغم ذيوع مسمي "الحرب الإلكترونية" إعلاميا، فإنه يعد مصطلحا قديما كان بالأساس مقصورا على رصد حالات التشويش على أنظمة الاتصال، بينما يكشف الواقع الراهن في الفضاء الإلكتروني عن دخول شبكات الاتصال والمعلومات إلى بنية ومجال الاستخدامات الحربية. مع تمدد الأعمال العدائية الإلكترونية إلى البنية التحتية المعلوماتية للدول لتحقيق أغراض متداخلة (سياسية، واقتصادية، وإجرامية، وغيرها)، حمل مفهوم الحرب الإلكترونية أبعادا جديدة، وصار البعض يفضل مصطلح "الحرب السيبرانية"، كتعبير عن ذلك التوجه الجديد، وإن ظلت لفظة "الحرب" ذاتها محل جدل، خاصة أن هناك مسميات عديدة تطلق على تلك الأنشطة العدائية الإلكترونية، منها، مثلا، الهجمات الإلكترونية، والإرهاب الإلكتروني، وغيرهما ، فوفقا للمفهوم التقليدي للحرب، فإنها تنطوي على استخدام الجيوش النظامية، ويسبقها إعلان واضح لحالة الحرب، وميدان قتال محدد، بينما تبدو هجمات الفضاء الإلكتروني غير محددة المجال، وغامضة الأهداف، كونها تتحرك عبر شبكات المعلومات والاتصالات المتعدية للحدود الدولية، إضافة إلى اعتمادها على

3- أثر الارهاب الإلكتروني على تغير مفهوم القوة في العلاقات الدولية ،ريهام عبدالرحمن رشاد العباسى ، (2001-2015) دراسة حالة: تنظيم "الدولة الاسلامية "نشرت بواسطة المركز الديمقراطي العربي قسم الدراسات الدينية و الجماعات الاسلامية قسم الدراسات المتخصصة، ص10،

4- حروب المستقبل، الهجوم الإلكتروني على برنامج إيران النووي ،عادل عبدالصادق، ، أبريل (2011) مجلة السياسة الدولية، مؤسسة الأهرام،

الإرهاب الإلكتروني: القوة في العلاقات الدولية ،نمط جديد وتحديات مختلفة ،عادل عبدالصادق، ، (2009) القاهرة: مركز الدراسات السياسية والاستراتيجية، الطبعة الأولي، ص155

أسلحة إلكترونية جديدة تلائم طبيعة السياق التكنولوجي لعصر المعلومات، حيث يتم توجيهها ضد المنشآت الحيوية، أو دسها عن طريق عملاء لأجهزة الاستخبارات.

لقد امتدت ساحات المعارك الحربية إلى الواقع الافتراضي الذي تحول لساحة حرب فعلية، تتعرض فيها الدول لخسائر اقتصادية و هزات اجتماعية و سياسية، و في هذا الشأن برزت أعمال القرصنة الإلكترونية بشكل كبير، فتعرضت ظاهرة الصراع إلى تغيرات مع بروز الفضاء الإلكتروني، كمجال تنشأ فيه نزاعات بين الفاعلين المختلفين و كحالة من التعارض في المصالح والقيم بين الفاعلين، سواء أكانوا دولا أم غير دول مما اوجب التفكير في الاستراتيجيات الحمائية، لما تنطوي تداعياته على مخاطر عدة على أمن الدول، سواء عن طريق التخريب، أو استخدام أسلحة الفضاء الإلكتروني المتعددة[5].

مع انتشار الفضاء الإلكتروني، وسهولة الدخول إليه، اتسعت دائرة الحروب و الهجمات الإلكترونية لتعبر عن الصراع الممتد بين الفاعلين المختلفين حول امتلاك أدوات الحماية والدفاع، وتطوير القدرات الهجومية الإلكترونية ،حيازة القوة، التفوق، الهيمنة، تعزيز التنافس حول السيطرة، والابتكار، والتحكم في المعلومات، وتعظيم القدرات على زيادة النفوذ والتأثير في المستويين المحلي والدولي[6]. انتقلت جبهات القتال بشكل مواز إلى ساحة الفضاء الإلكتروني وكان لهذا التغيير دورا في إعادة التفكير في حركية وديناميكية الصراع، بل وبروز ما يعرف بـ"عصر القوة النسبية و تعني هذه الأخيرة أن "القوة العسكرية" قد لا تكفي وحدها لتأمين البنية التحتية للدول، الأمر الذي يخلف آثارا استراتيجية هائلة على مستوي تركيبة وتوازنات النظام الدولي .

مع هذا التغير، أصبحت أهداف الحرب أقل مادية، وتركزت أكثر على العامل النفسي والدعائي، لاسيما مع تنامي التغطية الإخبارية، والسمعية، والبصرية المباشرة للأحداث لحظة وقوعها عبر مواقع الإنترنت والفضائيات، وضعف سيطرة أنظمة الحكم على توجهات مواطنيها[7].أسهم الفضاء الإلكتروني في دعم الهياكل التنظيمية والاتصالية للحركات والجماعات المحلية، والمنظمات المدنية، بما ساعد الفاعلين من غير الدول على ممارسة قوة التجنيد، والحشد، والتعبئة، واستجلاب التمويل. وهنا، تختلف أهداف الحروب الإلكترونية وفقا لطبيعة أهداف الصراعات وذلك على النحو الآتي:

1– طبيعة سياسية، باستخدام قدرات هجومية ودفاعية عبر الفضاء الإلكتروني بهدف إفساد النظم المعلوماتية، والشبكات والبنية التحتية لتحقيق أهداف سياسية.[8]

2– طبيعة ناعمة، للحصول على المعلومات، والتأثير في المشاعر والأفكار، وشن حرب نفسية وإعلامية. ويتم ذلك من خلال تسريب المعلومات، واستخدامها عبر منصات إعلامية، بما يؤثر في طبيعة العلاقات الدولية، كالدور الذي لعبه موقع ويكيليكس في الدبلوماسية الدولية[9].

5- اثر الارهاب الإلكتروني على مبدأ استخدام القوة في العلاقات الدولية(2001- 2007) عادل عبدالصادق الجخة،(2009)، مرجع سابق نص 156

6- الفضاء الإلكتروني وأنماط التفاعلات الدولية: دراسة في أبعاد الأمن الإلكتروني ،نوران شفيق على،(2014)، ،(ماجيستير)، جامعة القاهرة، كلية الاقتصاد والعلوم السياسية. ،ص108

7- روسيا تشن حربها السيبرانية على الغرب «ديفينس وان علاء الدين أغا، »، 2017/6/1، مركز البديل للتخطيط والدراسات الاستراتيجية، الرابط. http // el - badil-pss.org

8- الموسوعة الجزائرية للدراسات السياسية الاستراتيجية ، ايهاب شوقي (2017)www.politics-dz.com

3–الطابع التنافسي للاستحواذ على سباق التقدم التكنولوجي، وسرقة الأسرار الاقتصادية والعلمية. وقد يمتد إلى محاولة للسيطرة على الإنترنت، وعناوين المواقع، والتحكم بالمعلومات، والعمل على اختراق الأمن القومي للدول.

لصعوبة الفصل بين أنشطة الاستخبارات، وجمع المعلومات، وحروب الفضاء الإلكتروني، أو التمييز بين الاستخدام السياسي والإجرامي، فان الفضاء الإلكتروني يعد بيئة أكثر مناسبة للصراعات المعلوماتية، إذ يسهم في دعم قدرة الأجهزة الأمنية للدول، لصعوبة الرقابة التقليدية على التفاعلات الإلكترونية.

بهدف تحقيق "الهيمنة الإلكترونية الواسعة"[10]،فالحرب الجديدة لا تخضع لسيطرة الدول و اجهزتها الامنية و لا تعرف باتفاقيات و لا مواثيق و لا عهود دولية انما تفرض ضرورة التنسيق الدولي لا مننتها .

إن البيئة الجديدة للمجال الافتراضي و التي أصبح مصير الدول و مستقبلها مرهونين بقدرتها على التعامل معها، تتطلب العمل على استثمارها لإعادة تشكيل مفردات المنظومة الامنية .

4–القرصنة الإلكترونية

شهدت ساحة الحرب في "المجال الافتراضيِّ" Cyberspace العديد من التطورات و التجاذبات الميدانية و النظرية وتقف عمليات القرصنة الإلكترونية على رأس تلك الهجمات التي بدأت تثير قلق الدول والحكومات و تؤثر على امن الفضاء الالكتروني [11]

أ–ماهية عمليات القرصنة الالكترونية:هي عمليات اختراق إلكترونية موجهة سياسيا من دولة ما بهدف التجسس على شبكة حواسيب هيئات رسمية أو شركات خاصة كبرى في دولة أخرى، أو تخريب وتعطيل تلك الشبكات وما يرتبط بها من أجهزة، وهي شكل من أشكال حرب المعلومات[12]

يقوم بعمليات القرصنة إما أفراد أو شبكات خاصة من المحترفين أو أشخاص يعملون بشكل رسمي ضمن مؤسسات دولهم [13]

ب– الاستخدام السياسي لعمليات القرصنة الالكترونية

تستخدم عمليات القرصنة الإلكترونية على أكثر من مستوى، و منها اختراق الدولة وتدخلها في إحدى دول جوارها و التي قد تكون على خلافات معها أو تتدخل في قضايا ذات طابع إقليمي، وصولا إلى توظيف عمليات القرصنة على المستوى الدولي و استخدامها بين الدول الكبرى.

9– موقع ويكيليكس و تحدي عالم الاستخبارات الامريكي، عادل عبد الصادق، (2010)مركز الاهرام للدراسات السياسية و الاستراتيجية، ص 4

10– الهجمات عبر الانترنت، ساحة الصراع الالكتروني الجديدة ،محمد خالد وليد (2013)، المركز العربي للأبحاث و دراسة السياسات الدوحة قطر ،ص17

11– آفاق الأمن الإسرائيلي: الواقع والمستقبل ،خالد وليد محمود ، (2007)مركز الزيتونة للدراسات و الاستشارات ، الاردن ص 3

12– المشكلات الهامة في الجرائم المتصلة بالحاسوب الالي وابعادها الدولية ، دراسة مقارنة عامر الفاروق(1995) ، مصر ، ط 2،.ص 22

13– موقع ويكيليكس و تحدي عالم الاستخبارات الامريكي ،مرجع سابق ص 4

أثرت عمليات القرصنة بشكل سياسي على العلاقات بين الدول إذ أضحت العديد من الدول لا تثق ببعضها البعض وتتخوف من جيرانها بسبب الفضاء الرقمي، ولمحاولة الدول تحصين نفسها من مثل هذه الهجمات دشنت مؤسسات وجيوشا الكترونية خاصة لمثل هذه الأهداف تحقيقا للأمن الالكتروني .

أعلنت ألمانيا مثلا في أبريل 2017 عن تكوين جيش إلكتروني كوحدة مستقلة داخل الجيش إلى جانب القوات البرية والبحرية والجوية، حيث يمارس مهام دفاعية وهجومية على شبكة الإنترنت ولن يقتصر على صد هجمات القرصنة، بل سيرد عليها في ساحة المعركة، [14].

يتطلب مواجهة القرصنة تعاونا دوليا من خلال اتفاقية دولية لتطبيق القانون وتشديد العقوبات والتعاون مع منظمة التجارة العالمية، إضافة إلى تحديد الحكومات خسائر القرصنة و العمل على وضع أنظمة تشريعية متطورة لتنظيم البيئة القانونية والتنظيمية التي تخدم أمن تقنيات ونظم المعلومات، إلى جانب تطوير برمجيات آمنة ونظم تشغيل قوية تحد من الاختراقات الإلكترونية وبرمجيات الفيروسات وبرامج التجسس وذلك بشكل مستمر[15].

المبحث الثاني

إشكاليات المجتمع الدولي في التعامل مع الأسلحة الإلكترونية

اولا : بشأن القرصنة الإلكترونية العكسية.

تسعى الشركات الأمنية والحكومات بشكل دؤوب نحو ابتكار أدوات ووسائل جديدة لمنع عمليات القرصنة والتصدي لها، يقترح البعض الآخر الانتقال من موقع الضحية إلى موقع المهاجم، وذلك من خلال اتخاذ زمام المبادرة ومهاجمة القراصنة أنفسهم، بما يمكن وصفه "بالقرصنة العكسية"، ويفضل ديتريش [16]اللجوء إلى طرق أكثر ذكاء وسلمية عند تنفيذ "القرصنة العكسية" بحيث لا تتسبب بتعطيل حاسوب المهاجم، بل يتم الوصول إلى بياناته الخاصة والتعرف على الأدوات التي يستخدمها، ومعرفة الأشخاص المتعاونين معه، وغير ذلك من الأساليب التي قد توفر حلولا تساعد على التصدي للهجمات المستقبلية وتقليل فاعليتها.

يتنافى مفهوم "القرصنة العكسية" مع القوانين الدولية، حيث انه ووفق العديد من الخبراء الأمنيين– أن تنفيذ عمليات "القرصنة العكسية" لن يؤدي إلى النتائج المرجوة، ولن يساعد على تقليل نسب الهجمات الإلكترونية، خاصة فيما إذا كان الهدف من وراء تلك العمليات هو تعطيل الحواسيب المستخدمة بالهجمات فحسب، ووفقا للكاتب جفري كار مؤلف كتاب "داخل الحرب الإلكترونية"، فإنه بإمكان أي دولة شن حرب إلكترونية على دولة أخرى بغض النظر عن مواردها، وذلك لأن معظم القوات العسكرية ترتبط بشبكات حاسوبية وتتصل بالإنترنت، ولذلك فهي ليست آمنة، وللسبب ذاته بإمكان الجماعات غير الحكومية وحتى الأفراد شن هجمات حرب إلكترونية[17].

14- https //m/hespress.com06-04-2017

15- التوظيف السياسي لأعمال القرصنة الإلكترونية و أثرها على استقرار العلاقات الدولية ،محمد عامر (2017)مركز البديل للتخطيط والدراسات الاستراتيجية ص 3

16-مدير الاستخبارات الوطنية الامريكية(8 201-03-25) aljazeera.net

17- الجزيرة نت، الرابطaljazeera.net عندما يصبح الحاسوب فتاكا، الحرب الإلكترونية.. (2017/05/14).-

وحاليا فإن ثمة سباق بين الدول الغنية لتطوير برمجيات يكون من شأنها امتلاك قدرات هجومية وأخرى دفاعية قادرة على التصدي لأي هجمات و كإحدى أهم أدوات تحقيق السياسات الخارجية للدول، والداخلية أيضا وذلك بالتوازي مع الأشكال التقليدية للقوة، سواء كانت الصلبة أو الناعمة[18].

ثانيا: بشأن مرتكزات أمن الفضاء الإلكتروني

لقد أصبحت أخبار الاختراقات الإلكترونية وعمليات القرصنة عبر شبكة الإنترنت من أهم المواضيع التي تتصدر صفحات المواقع الإخبارية والتقنية، خاصة ،بعد تعرض جهات متنوعة وشركات كبرى لاختراقات أمنية ومن ثم يعتبر تأمين المعلومات والشبكات أكثر الطرق فعالية للحماية من الهجمات الإلكترونية[19].

حتى وقت قريب كان الأمن الإلكتروني حكرا إلى حد كبير على مجموعة صغيرة من خبراء الحاسوب لكن أصبحت حاليا شبكة الإنترنت الركيزة الأساسية للاقتصاد العالمي والحوكمة في مختلف أنحاء العالم، فدرجت قضية امن الفضاء الإلكتروني في استراتيجيات الأمن القومي للعديد من الدول من اجل الاستحواذ على مصادر القوة داخل الفضاء الإلكتروني و للعمل على الحيلولة دون تعرض بنيتها التحتية الحيوية للخطر الذي ينجم جراء قطع خدمة الإنترنت أو ضرب مواقعها.

لقد أصبح للأمن الإلكتروني تأثيرا عميقا على المجتمع والاقتصاد على النطاق الدولي[20]فهو يرتكز على مفاهيم ذات نطاق وطني وإقليمي وعالمي، ومفاهيم أخرى ذات أبعاد أمنية، وتكنولوجية، واقتصادية وسياسية، واجتماعية، وعسكرية...الخ لذا تزايدت العلاقة بين الأمن والتكنولوجيا، خاصة مع إمكانية تعرض المصالح الاستراتيجية للدول إلى أخطار وتهديدات، الأمر الذي حول الفضاء الإلكتروني لوسيط ومصدر لأدوات جديدة للصراع الدولي.

فرضت تلك التطورات إعادة التفكير في مفهوم "الأمن القومي للدولة"، والذي يعنى بحماية قيم المجتمع الأساسية، وإبعاد مصادر التهديد عنها، وغياب الخوف من خطر تعرض هذه القيم للهجوم[21] ، وبات توافر أمن الفضاء الإلكتروني يتحقق حال وجود إجراءات الحماية ضد التعرض للأعمال العدائية، والاستخدام السيئ لتكنولوجيا الاتصال والمعلومات، بيد أن طبيعة ذلك الفضاء، كساحة عالمية عابرة لحدود الدول، جعل الأمن الإلكتروني يمتد من داخل الدولة إلى النظام الدولي ليشكل نوعا من الأمن الجماعي العالمي، خاصة مع وجود مخاطر تهدد جميع الفاعلين في مجتمع المعلومات العالمي ،فأصبحت هناك مصلحة قطرية، وكذلك دولية، في الحفاظ على أمن الفضاء الإلكتروني، على أساس أن هذا الأخير صار جزءا من الأمن العالمي، بفعل الطبيعة المتغيرة للتفاعلات الإلكترونية، خاصة مع تطور القدرات البشرية على إنتاج تقنيات جديدة، فضلا عن تصاعد مخاطر التهديدات الإلكترونية على البنية التحتية الكونية للمعلومات.

لم يقتصر الاهتمام بالأمن الإلكتروني على البعد التقني فحسب، بل تجاوزه إلى أبعاد أخرى ذات طبيعة ثقافية، واجتماعية، واقتصادية، وعسكرية، وغيرها، خاصة أن الاستخدام غير السلمي للفضاء الإلكتروني يؤثر في الرخاء .ان استراتيجية مواجهة القوة الذكية ، تفرض

18- كيف يمكن أن تدير الدول شؤونها في عصر الإنترنت، إيهاب خليفة القوة الإلكترونية، ، وحدة التطورات التكنولوجية بمركز المستقبل للأبحاث والدراسات،

19- الجرائم المعلوماتية على شبكة الأنترنت، أمير فرج يوسف ، (2009)، دار المطبوعات الجامعية ، الإسكندرية ،ص 21

20- رؤية استراتيجية لحماية الفضاء الالكتروني للملكة العربية السعودية ، مرجع سابق ،ص 8

21- مفهوم الأمن في مرحلة ما بعد الحرب الباردة، مصطفي علوي، ، أبحاث المؤتمر الذي عقده مركز الدراسات الآسيوية 4-5 مايو 2002: قضايا الأمن في آسيا، تحرير: هدي ميتكيس، والسيد صدقي عابدين،(2004) (القاهرة: كلية الاقتصاد والعلوم السياسية، مركز الدراسات الآسيوية ،ص14

تطور النظام الدولي لتحقيق مسؤولية اكبر في النظام العالمي الاقتصادي، والاستقرار الاجتماعي لجميع الدول التي أصبحت تعتمد بنيتها التحتية على الفضاء الإلكتروني[22].

ثالثا: صعوبات تطبيق القانون الدولي لتوفير الامن الالكتروني

تبلورت مصالح قومية للدول في الفضاء الإلكتروني، إثر تزايد الاعتماد على ربط البني التحتية لها بذلك الفضاء في بيئة عمل تشابكية واحدة، تعرف بـ "البنية التحتية القومية للمعلومات وبالتالي، فأي تهديد محتمل أو هجوم على إحدى تلك المصالح أو كلها للدولة قد يشكل مدعاة لحدوث عدم توازن استراتيجي، وهو ما يكشف عن نمط جديد من التهديدات للأمن القومي للدول.

أدي اتساع علاقة الدول بالفضاء الإلكتروني، إلى جملة من المخاطر والتداعيات على تفاعلات السياسة الدولية، يمكن طرح أبرزها على النحو الآتي:

1- تصاعد المخاطر الإلكترونية، خاصة مع قابلية المنشآت الحيوية (مدنية وعسكرية) في الدول للهجوم الإلكتروني عليها عبر وسيط وحامل للخدمات وإن التحكم في تنفيذ هذا الهجوم يعد أداة سيطرة استراتيجية بالغة الأهمية، سواء في زمن السلم أو الحرب [23]

2- تعزيز القوة وانتشارها، فمن جهة، عزز الفضاء الإلكتروني ما يسمي بـ "القوة المؤسسية" في السياسة الدولية، وهي تعني أن يكون لها دور في قوة الفاعلين، وتحقيق أهدافهم وقيمهم في ظل التنافس مع الآخرين، والإسهام في تشكل الفعل الاجتماعي في ظل المعرفة والمحددات المتاحة، والتي تؤثر في تشكيل السياسة العالمية ،من جهة أخرى، عمل الفضاء الإلكتروني على إعادة تشكيل قدرة الأطراف المؤثرة، فبرزت عملية انتشار القوة بين أطراف متعددة، سواء أكانت دولا، أم من غير الدول.[24]

3- عسكرة الفضاء الإلكتروني، وذلك سعيا لدرء تهديداته على أمن الفضاء الإلكتروني، وبرز في هذا الإطار اتجاهات، للتطور في مجال سياسات الدفاع والأمن الإلكتروني، وتبني سياسات دفاعية .

4-إدماج الفضاء الإلكتروني ضمن الأمن القومي للدول، وذلك عبر تحديث الجيوش، وتدشين وحدات متخصصة في الحروب الإلكترونية، إجراء المناورات لتعزيز الدفاعات الإلكترونية، والعمل على تعزيز التعاون الدولي في مجالات تأمين الفضاء الإلكتروني، والقيام بمشروعات وطنية للأمن الإلكتروني.

5 -تحديث القدرات الدفاعية والهجومية، حيث سعت الدول إلى تحديث النشاط الدفاعي لمواجهة مخاطر الحرب السيبرانية، والاستثمار في البنية التحتية المعلوماتية، وتأمينها، وتحديث القدرات العسكرية، ورفع كفاءة الجاهزية وهنا، يتعلق التوجه الأخطر بنقل تلك القدرات من الدفاع إلى الهجوم عن طريق استخدام تلك الهجمات في إطار إدارة الصراع والتوتر مع دول أخرى [25] هذا و تنطوي عملية بناء القدرات العسكرية في مجال الأسلحة الإلكترونية على عناصر أساسية، منها :

22- هل تحتاج امريكا الى اكتشاف كيف تكون قوة ذكية ، جوزيف اسي ناي ، (10-03-2018) إميل أمين مستقبل القوة ، جريدة عمان

23- الفضاء الإلكتروني والعلاقات الدولية: دراسة في النظرية والتطبيق، عادل عبدالصادق، (2016) المكتبة الأكاديمية، القاهرة، ص 22

24- الإرهاب الإلكتروني: القوة في العلاقات الدولية .. نمط جديد وتحديات مختلفة ،عادل عبدالصادق، (2009) ، مركز الدراسات السياسية والاستراتيجية، القاهرة ، الطبعة الأولي، ص155

25- القوة الإلكترونية: أسلحة الانتشار الشامل في عصر الفضاء الإلكتروني ،عادل عبدالصادق،(2012)، مجلة السياسة الدولية، العدد 188

– السعي إلى امتلاك التكنولوجيا، وأنظمة الحماية، وتطوير قدرات هجومية تعمل على تحقيق التفوق التقني،

– تطوير القدرات الهجومية، إما عبر بناء القدرات الذاتية، أو بالاستعانة بالأفراد والشركات المتخصصة، وتطوير القدرة على اختبار مدي الجاهزية لمواجهة الهجمات الإلكترونية[26]

– العمل على توفير الميزانيات المخصصة لتطوير القدرات الهجومية والدفاعية، وخاصة مع قلة تكلفتها، مقارنة بحجم ما ينفق على الجيوش التقليدية.

و عموما تتمثل متطلبات توافر الأمن الإلكتروني الدولي في التأكد من سلامة الدفاعات الإلكترونية، وعدم تعرضها لأي خلل فني طارئ، وألا تعالج هذه المسألة منفصلة عن غيرها، وإنما ضمن ترسانة شاملة للدفاع عن أي حرب استباقية.[27]

و لكن و رغم تزايد الوعي بأهمية الأمن الالكتروني، فإن إمكانيات تطبيق القانون الدولي لتنظيم سلوك الدول لتوفير الامن الالكتروني ،ظلت محدودة وقد دارت عدة نقاشات بشأن قدرة القانون الدولي على ضبط أنشطة الدول في هذا المجال ،ومن أهم الإشكاليات التي تواجه المجتمع الدولي في طريقة التعامل مع الأسلحة الإلكترونية ، ما يتعلق بالجدل حول مدى اعتبار الأسلحة الإلكترونية مثل الأسلحة غير التقليدية وإمكانية أن تخضع لقيود اتفاقيات الحد من التسلح وهو ما يقابل بأن الفاعلين في مثل تلك الأسلحة ليسوا بدول بالضرورة ومن ثم لن يخضعوا للالتزام بالاتفاقيات الدولية، و مدى اعتبار الهجوم الإلكتروني هجوما مسلحا وفق القانون الدولي ومتى يتم اعتباره كذلك في حالة تحديد المسؤولية حول من قام بالهجوم.

عموما يمكن القول ايضا أنه في حالة استخدام الأسلحة الإلكترونية يصعب تحديد من المسئول عن هجماتها كما ان الدول لا تستجيب في الغالب لعرض قدراتها الإلكترونية من الأسلحة دون أية ضمانات والتي تعتمد بالأساس على الابتكار ،البحث ،التطوير والسرية[28].

المبحث الثالث

مضمون الرؤية الشاملة لمستقبل التعاون الدولي المتعلق بالأمن الإلكتروني

تلقى قضية أمن الفضاء الالكتروني اهتماما متصاعدا على أجندة الامن الدولي وذلك في محاولة لمواجهة تصاعد التهديدات الالكترونية ودورها في التأثير على الطابع السلمي للفضاء الالكتروني و ساهمت تلك المتغيرات في بروز وعي عالمي بما يحدث و درجة عالية من التأثير والتأثر في أرجاء العالم المختلفة ،وأفرز الفضاء لإلكتروني بيئة دولية جديدة تمثلت في إعطاء دفعة قوية لزيادة المعرفة و الحماية الالكترونية .

اولا : الجهود الدولية لمواجهة الاختراقات الإلكترونية

26 – الهجمات عبر الإنترنت: ساحة الصِّراع الإلكترونيِّ الجديدة، خالد وليد محمود ، المركز العربي للأبحاث و دراسة السياسات ،الدوحة قطر ،ص 7

– فواعل افتراضيَّةٌ: المواجهات الإلكترونيَّة بين القوى السِّياسيَّة بعد الثَّورات العربيَّة، نوران شفيق علي، (2013)، مجلة السياسة الدولية، 10 http://www.siyassa.org.eg/NewsContent/2/106/3137

27– كيف يمكن الاستعداد "لليوم الأسود" في الإنترنت؟، إيهاب خليفة،(2017/5/17) مركز المستقبل للأبحاث والدراسات المتقدمة، التحليلات التطورات التكنولوجية https // futureuae.com

28– استخدام القوة الالكترونية في ادارة التفاعلات الدولية: الولايات المتحدة نموذجاً 2001– 2012، ايهاب عبدالحميد خليفه عبدالعال،(2015)،مرجع سابق ص 10

أدي تصاعد المخاطر والتهديدات في الفضاء الإلكتروني إلى بروز تنافس بين الشركات العاملة في مجال الأمن الإلكتروني بغرض تعزيز أسواق الإنفاق العالمي على تأمين البني التحتية للدول، بالإضافة إلى بروز فاعلين آخرين من شبكات الجريمة المنظمة والقراصنة و منه ظهرت الحاجة إلى تطوير استراتيجيات جديدة تتلاءم مع العصر الذي اختلفت فيه حسابات القوة والردع والحرب، العصر[29] الذي أصبحت فيه الإنترنت الإطار العام الحاكم لكافة تفاعلاته، سواء كانت شخصية أو عامة، عسكرية أو سياسية، اقتصادية أو اجتماعية، بهدف معرفة التغيرات التي طرأت على مفاهيم القوة وممارسة النفوذ في العلاقات الدولية بفضل الإنترنت، وكيف أصبحت مصدر تهديد للدول والأفراد، ومعرفة المخاطر التي يمكن أن يتعرض لها الأمن القومي للدول .

إن آلية المواجهة للاختراقات الإلكترونية أمرا مثيرا للجدل، وإن كانت مواجهة عملية القرصنة عبر تعزيز إجراءات الحماية الرئيسية للبنية الرقمية والتكنولوجية في الدول من الاختراق واتخاذ إجراءات[30] تستهدف ردع المخترقين تحظى بشبه اتفاق ، وبالرغم من هذا الجدل، يمكن التعرف على اتجاهين للمواجهة [31]

– الحماية والردع الإلكتروني حيث سعت الحكومات مؤخرا إلى تشديد إجراءات الرقابة من أجل مواجهة عمليات القرصنة الإلكترونية على بنيتها الأساسية الرقمية، وعززت تلك الإجراءات بالإعلان عن خطوات ردع

– وقف تدفق المعلومات المضللة عبر الشفافية والتحقق، ففي مواجهة انتشار المعلومات المضللة والبروباجندا[32] سعت مؤسسات وشركات داخل الولايات المتحدة وألمانيا إلى تطوير تكنولوجيات أسمتها Fact checker، مثل المشروع الذي أطلقته جامعة بنسلفانيا مؤخرًا، وهو مشروع تفاعلي يتيح للجمهور إرسال الأخبار المشكوك فيها، والسعي للتحقق من صحتها، عبر ترميزها أو إرسالها من قبل الجمهور إلى جهات محايدة تتولى القيام بعملية التحقق تلك.

1– جهود الأمم المتحدة

ورغم أن المعايير الدولية تميل إلى التطور ببطء فقد عكفت مجموعة الأمم المتحدة للخبراء الحكوميين على تحليل كيفية ارتباط القانون الدولي بالأمن الإلكتروني و قد ساعدت تقارير فريق الخبراء الحكوميين التابع للأمم المتحدة في أعوام 2010، و2013، و2015 على وضع جدول أعمال المفاوضات حول الأمن الإلكتروني، وآخرها تحديد مجموعة من المعايير التي أقرتها الجمعية العامة للأمم المتحدة و منها ما تضمنه القرار رقم 167/68 المتعلق بالحق في الخصوصية في العصر الرقمي .

29– الانترنت والجوانب القانونية لنظم المعلومات، محمد السعيد رشدى ، (15–14مارس 1999) بحث مقدم إلى المؤتمر العلمي الثاني لكلية الحقوق، جامعة حلوان بعنوان الاعلام والقانون. ص 3

30قضايا استراتيجية تحديات القوانين: الفضاء الافتراضي والقانون الدولي، الياس الصديقي – 25 نوفمبر 2017 دوريات

31– فواعل افتراضيَّةٌ: المواجهات الإلكترونيَّة بين القوى السِّياسيَّة بعد الثَّورات العربيَّة" نوران شفيق علي، مجلة السياسة الدولية، 10 حزيران/ يونيو 2013http://www.siyassa.org.eg/NewsContent/2/106/3137

32 –الهجمات السيبرانية ،رغدة البهي ، (2017)مجلة العلوم السياسية و القانون بكلية الاقتصاد و العلوم السياسة جامعة القاهرة العدد الاول ، المركز الديمقراطي العربي

و مع ذلك فقد تم تحقيق أكبر قدر من التوافق النسبي[33] في مسالة اعتماد الدول الاتفاق حول المجال الالكتروني في عام 2015 عندما وضعت مجموعة من الخبراء امن المعلومات الدولي في الامم المتحدة تضم 20 دولة اساسا لنوع من اتفاق عالمي على عدم الاعتداء الالكتروني و وفقا للاتفاق :

1- تتعهد الدولة باستخدام التقنيات الالكترونية حصرا لأغراض سلمية و عدم مهاجمة البنية التحتية الحساسة ،

2-التوقف عن ادراج البرمجيات الخبيثة في المنتجات التي تنتجها تكنولوجيا المعلومات

3-الامتناع عن تراشق التهم العشوائي بشان المسؤولية عن الهجمات الإلكترونية

4-بذل جهود لمكافحة المتسللين

بيد ان هذا الاتفاق يخلو من كل درجات الالزامية ،فمعايير مجموعة الامم المتحدة في هذا الاطار لا تزال طوعية

2-جهود المنظمات الحكومية وغير الحكومية

تم إطلاق العديد من المبادرات التي تقوم بها المنظمات الحكومية وغير الحكومية لدعم الأمن الإلكتروني:

- الاتحاد الدولي للاتصالات:أثرت التطورات التي عرفتها وسائل الاتصال في العلاقات الدولية تأثيرا بالغا فقد عملت هذه التطورات التكنولوجية الحديثة على إزالة الفوارق والحدود التي فصلت بين الدول والقارات، فعملت على تقريب الشعوب من بعضهم البعض ما نتج عنه نضوج أكبر للأفكار وسرعة في تبادل وانتقال المعلومات[34]

فتكنولوجيا الاتصال الحديثة تتمثل في تلك العملية الاجتماعية التي يتم فيها استخدام عدد من الوسائل المادية و المعارف الذهنية في مختلف عمليات الاتصال الإنتاج و التنظيم التي تسمح للمستخدم بالولوج إلى مجموعة غنية من التطبيقات من أجل تحقيق أهداف و غايات محددة، سمتها الأساسية الدمج بين الوسائل التقليدية و الحديثة على السواء و يمكن القول أن تكنولوجيا الاتصال الحديثة تتمتع بخصائص يمكن حصرها في التفاعلية، التنوع، التكامل ، تجاوز الحدود الثقافية و الكونية،[35] و تؤكد اقامة الشركات العالمية الدور الذي يضطلع به الاتحاد كمحفز عالمي للتعاون الدولي في مجال الامن الإلكتروني الذي يؤكد انه لا يمكن تنفيذ الامن الالكتروني على المستوى الوطني بدون اعتماد التشريعات الملائمة .

-حلف شمال الاطلسي -الناتو

33- تأثير تكنولوجيا الاتصال الحديثة على العلاقات الدولية، مريم شوقي(18 / 1 / 2014) الحوار المتمدن-العدد: 4338 -ا مواضيع وابحاث سياسية

34 - La cyber sécurité au cœur r du forum mondial des politiques de télécommunication 16-05-2013 https://news.Un.org

35- واقع استخدام التكنولوجيات الحديثة للإعلام و الاتصال في الصحافة المكتوبة بالجزائر، فريد بن زايد،(2009-2010)ماجستير في علوم الإعلام و الاتصال تخصص اتصال و علاقات عامة، قسنطينة ،ص 48.

أنشأ وحدة للدفاع الإلكتروني من خلال محتوى دليل "تالين للقانون الدولي في الحرب الإلكترونية، الذي يجيب على أهم النقاط الأساسية ذات الصلة بالحروب والهجمات الإلكترونية التي تنفذها الدول، أو تلك التي تقوم بها جهات فاعلة من دون الدول، وكذا مفهوم النزاع المسلح في إطار الحرب الإلكترونية و ضرورة مراعاة مبادئ القانون الدولي الإنساني المعروفة كمبدأ التمييز مثلا، ومسألة شرعية استهداف المقاتل الإلكتروني.يعد دليل "تالين للقانون الدولي في الحرب الإلكترونية، صك قانوني اعد عام 2013 من قبل مجموعة من خبراء القانون الدولي بدعوة من حلف شمال الاطلسي الناتو،حيث أوجدت هذه الوثيقة معايير دولية لاستعمالات الأسلحة الرقمية من خلال القواعد التالية :

القاعدة1 –تمارس الدولة رقابتها على المنشآت الالكترونية في اطار سيادتها الاقليمية

القاعدة2– تمارس الدولة اختصاصها على الاشخاص الممارسين للأنشطة الالكترونية داخل اقليم الوطن

القاعدة4–اي تدخل لدولة ما في المنشآت الالكترونية لدولة اخرى يعد خرقا لسيادتها

القاعدة 6– تتحمل الدول المسؤولية القانونية عن انشطتها الالكترونية التي تخترق بموجبها اي التزام دولي

القاعدة32– المتعلقة بحضر مهاجمة المدنيين، ولقد اكدت الكثير من الدراسات بان هذه الوثيقة هي الوحيدة المعبرة عن تكيف القانون الدولي الحالي مع الحروب الالكترونية [36]

–الاتـحاد الأوروبي

من خلال مضامين الاتفاقية الاوروبية لمكافحة جرائم الانترنت بودابست 2001 حاول الاتحاد تطبيق سياسة التعاون للأمن و الدفاع في الفضاء الرقمي و في عام 2018 سعت الدول الاوروبية الى الاتفاق من اجل :–انشاء نظام اصدار شهادات الأمن الإلكتروني

–انشاء وكالة الامن الالكتروني باختصاصات و صلاحيات اوسعه في مجال الامن الالكتروني لتقديم المساعدة للدول التي تتعرض لهجمات إلكترونية [37]

– مجموعة السبعة

اكدت في اجتماعها في ايطاليا في شهر افريل 2017، على ان القلق يتزايد من التلاعب الرقمي المحتمل حدوثه في العمليات السياسية الديمقراطية. و قد تبنت الولايات المتحدة، "الاستراتيجية الدولية للفضاء الإلكتروني" وهي أول وثيقة سياسية من هذا النوع، تبين الرؤية الشاملة لمستقبل التعاون الدولي المتعلق بالفضاء الإلكتروني.

3– المؤتمرات الدولية

- المؤتمر العالمي للفضاء السيبراني (الإلكتروني) بهولندا لعام 2015

36ماهية الحرب الالكترونية في ضوء قواعد القانون الدولي، سعيد درويش،كلية الحقوق حوليات جامعة الجزائر العدد 29 الجزء الثاني ص،115

37 - La coopération internationale et bilatérale enjeux et rivalités, DesForges Alix, ,IRESM ,2013,No16,18

-مؤتمر الحروب المستقبلية في القرن 21 الامارات العربية 2013

- قمة دبي 2009:الدفاع في الامن المعمق للكمبيوترات تناولت القرصنة المعلوماتية الهاكرز

عموما نقول ان هذه المبادرات لم تعرف نجاحا لأسباب منها ان الولايات المتحدة و الدول الاوروبية تعتبر أن تنظيم الامن الالكتروني والزام الدول به:

1-يشكل رغبة من الطرف الضعيف للحد من امكانيات الدول المتقدمة لتطوير تكنولوجياتها الهجومية

2-الامر يعد غير واقعي، لان الترتيبات التقليدية مثل معاهدة عدم انتشار الأسلحة النووية لن تكون فعالة في الفضاء الالكتروني

3- طلب اعتماد مبدأ عدم التدخل في الشؤون الداخلية للدول على شبكة الأنترانت يعد في نظر الدول القوية عنصر تحكم لتعزيز رقابة الدولة على الانترنت .

ثانيا–واقع تنظيم الامن الالكتروني في بعض التشريعات العربية :لقد قطعت بعض الدول العربية اشواط معتبرة في محاولة توفير تنظيما محكما بشأن الأمن الالكتروني، لبناها التحتية الاساسية الحيوية:

-المملكة العربية السعودية من خلال نظام مكافحة جرائم المعلوماتية و التعاملات الالكترونية لعام 2007

-الامارات العربية المتحدة قانون الاتحاد لعام 2006 في شان مكافحة جرائم تقنية المعلومات

- الجزائر عمدت الى وضع مقاربة وطنية "شاملة للوقاية من القرصنة الالكترونية وحماية المؤسسات والهيئات العمومية و توفير الأمن الالكتروني ، بالزام السلطات العمومية ، على تطوير هذا التصور و تعميمه على مجموع الهيئات والمؤسسات الاقتصادية للقطاعين الخاص و العام .

كما بادرت بتطور مقاربة "دفاعية" من خلال اقتناء تجهيزات الحماية في حين أن المقاربة "الهجومية تعد "ضرورية" لمواجهة كل أشكال التهديدات التي تكمن في إنشاء دوائر لخبراء في المجال من خلال توعية مختلف الهيئات .

كما أصدر المشرع في الجزائر قانونا لحماية المعلومات وتأمين المعاملات لمواجهة أضرار القرصنة الإلكترونية [38]

يعد قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، خطوة نحو ردع جرائم المعلوماتية، خاصة ما تعلق منها بتسخير الوسيلة التكنولوجية للترويج للإرهاب والدعاية، وبذلك تكون الحكومة قد أخذت أول خطوة نحو سد الفراغ القانوني الذي كان موجودا في مكافحة الجريمة المعلوماتية.

ويعد هذا القانون الذي يأتي في سياق مكافحة الإرهاب الإلكتروني، بمثابة إطار قانوني مهم يحدد في بابه الأول تعريف وتحديد الجرائم

38- - القانون رقم 09-04 المؤرخ في 05اوت 2009 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها ، الجرية الرسمية عدد 47

- المرسوم الرئاسي رقم 15-261 الصادر في 5 اكتوبر سنة 2015 الذي يحدد تشكيلة و تنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها الجريدة الرسمية عدد53 صادر في 8 اكتوبر سنة 2015

المعلوماتية ثم ينتقل إلى إمكانية الحد منها ومواجهتها بعد أن أصبحت تلك الجرائم من بين الجرائم التي تهدد أمن وسلامة المجتمعات، حيث جاء في 19 مادة و6 فصول تؤكد في مجملها على احترام مبدأ المحافظة على سرية الاتصالات إلا في استثناءات حددها المشروع.و قدتم انشاء مركز وطني لمراقبة تدفق المعلومات ،الذي يضبط أكثر تبادل المعلومات ويحمي المشتركين من أي قرصنة من خلال جمعه لكل ممولي الانترنت و يعد مركزا ذكيا، يؤمن المعلومات من خلال وضع نقطة التقاء بين مختلف الممولين، لمراقبة المحتويات ومنع المواقع غير المرغوب فيها، سواء من قبل الممول أو من قبل الدولة التي لها الحق في الاطلاع على ما يجري عبر الشبكة العنكبوتية. تبنت الجزائر سياسة وطنية[39] لتشجيع هذه الأنظمة الحرة، ووضع مصلحة لأمن المعلومات والوقاية من الاختراقات والهجومات التي تهدد شبكات المعلوماتية الوطنية والتي تمس بوابات المواقع الجزائرية .

الخاتـــمة

يشهد العالم الآن ثورة تعتمد على المعلومات والمعرفة، ألا وهى الثورة التكنولوجية، التي لم يتم استخدامها في الأعمال السلمية فقط، ولكن تم استخدامها بشكل سلبي يضر بالبشرية بأكملها.

لذا فإن الصراعات التي يعرفها العالم ومحاولة تغيير موازين القوى بين مختلف التحالفات الدولية التي أخذ ت مسارا جديدا على شكل هجمات إلكترونية ، تفرض إعادة النظر في وضع استراتيجيات أمنية جذرية في النظم المعلوماتية ، مع الأخذ بعين الاعتبار أن الأنظمة الدفاعية التي يقدمها خبراء الأمن اليوم قد تشكل غدا ثغرات أمنية مقصودة إذا استوجب الأمر.

إن الفضاء الإلكتروني أصبح فعلا أحد الساحات الفعلية والفاعلة في إضعاف الدول لبعضها البعض وقد يتخطى مرحلة الحرب الباردة بكثير ليقترب من الحرب الساخنة إن لم يتسبب فيها بالفعل، وهذا ما يطرح تساؤلات حول ضرورة وضع اتفاقيات دولية تنظم الفضاء الإلكتروني و تعزز الامن الالكتروني ، إلى جانب دعم الدول لقدراتها الإلكترونية والتصدي لعمليات القرصنة سواء التي تنفذها دولا معادية لتحقيق أهداف اقتصادية وسياسية أو يقوم بها محترفون من أجل جمع الأموال والتخريب.

النتائـــج:

خلصت الدراسة الى جملة من النتائج نوجز اهمها فيما يلي :

1-يؤثر الامن الإلكتروني في القدرة التفسيرية والنظرية للعلاقات الدولية وفي بنية الأمن العالمي.

2-يشكل الفضاء الإلكتروني الساحات الفعلية والفاعلة في إضعاف الدول لبعضها البعض.

3- يعاني المجتمع الدولي من فراغ نظري على صعيد قوانين و احكام و شروط حرب الفضاء الالكتروني و الامن الالكتروني.

4-انعدام أعراف مشتركة تسهل الوصول إلى تفاهم بين الدول بالنظر إلى التحديات المرتبطة بالأمن الإلكتروني.

5- لا يزال النقاش دائرا حول المسائل القانونية المتعلقة بالهجمات الالكترونية المعاكسة، لان الرد الانتقامي يعد عملا عدوانيا مخالفا لقواعد القانون الدولي.

39- أعمال مؤتمر الجرائم الإلكترونية المنعقد في طرابلس/ لبنانK عاقلي فضيلة ، يومي 24-25|03|2017، ص 115.

6-تقع المسؤولية على المجتمعات الدولية للتصدي لمخاطر الهجماتالإلكترونية بالتوعية بمفهومها و مخاطرها

7-إن الوصول إلى استراتيجيات تضمن مواجهة الاختراقات الإلكترونية ، تفرض نشر المعلومات المسربة أو المضللة و تبني الحكومات تشريعات وسياسات تضمن شفافية المعلومات حول مصادر تمويل المواقع الإخبارية.

التوصيات:

1-تحديد جهات دولية تتولى وضع و تدقيق سياسات الامن الالكتروني (معايير و برامج).

2- الاتفاق دوليا او اقليميا على وضع أسس اكتشاف البرامج المشبوهة والتصدي لها.

3- ابرام اتفاقية دولية لمنع حرب الفضاء الالكتروني، بالموافقة على بروتكول دولي لوضع الاهداف المدنية في قائمة الاهداف التي يحضر على الدول استخدام الاسلحة الالكترونية ضدها .

4-إعتماد استراتيجية على مستوى كل دولة بأبعاد قانونية امنية ،أكاديمية ، اقتصادية ،اقليمية و دولية لمواجهة الهجمات الإلكترونية.

5- حث الدول على تطوير القدرات العسكرية الذاتية، للتكيف مع الواقع العالمي الراهن خصوصا على امتلاك قدرات دفاعية متقدمة في مجال الامن الالكتروني و المعلوماتية.

6- التزام كل دولة على حدى ببناء مضلة دفاعية متقدمة الكترونيا لحماية بناها التحتية الاساسية الحيوية.

7-الالتزام بالمفاهيم و المبادئ ثابتة في القانون الدولي ، خاصة فيما يتعلق بمبدأ السيادة و حالات شرعية لجوء الاطراف الى استخدام القوة او حق الدفاع.

8-وضع ضوابط تحكم السياسات و التفاعلات الدولية في اطار اعتماد قواعد سلوك الدول في الفضاء الالكتروني ، التزاما باتفاقية الامم المتحدة لضمان امن المعلومات الدولي.

9-ضرورة دمج مجال السبيرانية في البرامج الأكاديمية الجامعية على ان تصبح مادة تعلمية .

10 - انشاء وكالة دولية باختصاصات و صلاحيات اوسعه في مجال الامن الالكتروني لتقديم المساعدة للدول الفقيرة التي تتعرض لهجمات إلكترونية .

المراجـع

القوانين

1-نظام مكافحة جرائم المعلوماتية و التعاملات الالكترونية 2007 المملكة العربية السعودية.

2-قانون الاتحاد لعام 2006 في شان مكافحة جرائم تقنية المعلومات الامارات المتحدة.

3- القانون رقم 09-04 المؤرخ في 05اوت 2009 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها ، الجرية الرسمية عدد 47 .

4- المرسوم الرئاسي رقم 15-261 الصادر في 5 اكتوبر سنة 2015 الذي يحدد تشكيلة و تنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها الجريدة الرسمية عدد53 صادر في 8 اكتوبر سنة 2015.

الكـتب

1- الجرائم المعلوماتية على شبكة الأنترنت، أمير فرج يوسف (2009) دار المطبوعات الجامعية الإسكندرية .

2- المنازعات الدولية: مقدمة للنظرية والتاريخ، جوزيف س. ناي الابن، ترجمة: أحمد أمين الجمل، ومجدي كامل، الجمعية المصرية لنشر المعرفة والثقافة العالمية ،القاهرة.

3- الإرهاب الإلكتروني: القوة في العلاقات الدولية ، نمط جديد وتحديات مختلفة، عادل عبدالصادق(2009): مركز الدراسات السياسية والاستراتيجية، الطبعة الأولي، القاهرة .

4- المشكلات الهامة في الجرائم المتصلة بالحاسوب الالي وابعادها الدولية ،عامر الفاروق (1995) دراسة مقارنة ، مصر ، الطبعة الثانية .

5_ الفضاء الإلكتروني والعلاقات الدولية: دراسة في النظرية والتطبيق، عادل عبدالصادق (2016):المكتبة الأكاديمية القاهرة .

الرسائل العلمية

1- رؤية استراتيجية لحماية الفضاء الالكتروني للملكة العربية السعودية ،حامد ابن قنيفذ ونس الشمري (2015) ،(ماجيستير)جامعة نايف العربية للعلوم الامنية كلية العلوم الاستراتيجية.

2_ استخدام القوة الالكترونية في ادارة التفاعلات الدولية: الولايات المتحدة نموذجاً 2001- 2012،ايهاب عبدالحميد خليفه عبدالعال،(2015)، ،(ماجيستير)، جامعة القاهرة، كلية الاقتصاد والعلوم السياسية.

3- اثر الارهاب الإلكتروني على مبدأ استخدام القوة في العلاقات الدولية(2007 -2001) ،عادل عبدالصادق الجخة،(2009)،(ماجيستير)، جامعة القاهرة، كلية الاقتصاد والعلوم السياسية.

4 – الفضاء الإلكتروني وأنماط التفاعلات الدولية: دراسة في أبعاد الأمن الإلكتروني، نوران شفيق على،(2014)، (ماجيستير)، جامعة القاهرة، كلية الاقتصاد والعلوم السياسية.

5 – واقع استخدام التكنولوجيات الحديثة للإعلام و الاتصال في الصحافة المكتوبة بالجزائر، فريد بن زايد(2009) ،(ماجيستير) جامعة ،قسنطينة، الجزائر.

المؤتمرات والندوات العلمية

1- مفهوم الأمن في مرحلة ما بعد الحرب الباردة، مصطفي علوي،(2004) في أبحاث المؤتمر الذي عقده مركز الدراسات الآسيوية 4-5 مايو 2002: قضايا الأمن في آسيا، تحرير :هدي ميتكيس، والسيد صدقي عابدين ،القاهرة كلية الاقتصاد والعلوم السياسية، مركز الدراسات الآسيوية.

2- الانترنت والجوانب القانونية لنظم المعلومات ،محمد السعيد رشدى (1999) بحث مقدم إلى المؤتمر العلمي الثاني كلية الحقوق، جامعة حلوان بعنوان الاعلام والقانون..

3- الجرائم الإلكترونية، عاقلي فضيلة (2017)مؤتمر المنعقد في طرابلس/ لبنان.

الدوريات العلمية

1- كيف يمكن أن تدير الدول شؤونها في عصر الإنترنت ،إيهاب خليفة القوة الإلكترونية، وحدة التطورات التكنولوجية بمركز المستقبل للأبحاث والدراسات.

2- مستقبل القوة، إميل امين (2018) جريدة عمان ، هل تحتاج امريكا الى اكتشاف كيف تكون قوة ذكية ،جوزيف اسي ناي ، عرض و تحليل .

3- أثر الارهاب الإلكتروني على تغير مفهوم القوة في العلاقات الدولية، ريهام عبدالرحمن رشاد العباسي ، (2015) دراسة حالة: تنظيم "الدولة الاسلامية "نشرت بواسطة المركز الديمقراطي العربي قسم الدراسات الدينية و الجماعات الاسلامية قسم الدراسات المتخصصة.

4- حروب المستقبل .. الهجوم الإلكتروني على برنامج إيران النووي ،عادل عبدالصادق(2011) مجلة السياسة الدولية، مؤسسة الأهرام.

5- موقع ويكيليكس و تحدي عالم الاستخبارات الامريكي، عادل عبد الصادق(2010) مركز الاهرام للدراسات السياسية و الاستراتيجية.

6- الهجمات عبر الانترنت، ساحة الصراع الالكتروني الجديدة ،محمد خالد وليد (2013) المركز العربي للأبحاث و دراسة السياسات الدوحة قطر.

7- آفاق الأمن الإسرائيلي: الواقع والمستقبل ،خالد وليد محمود،(2007) مركز الزيتونة للدراسات و الاستشارات الاردن .

8- التوظيف السياسي لأعمال القرصنة الإلكترونية و أثرها على استقرار العلاقات الدولية، محمد عامر (2017)

9-فواعل افتراضية: المواجهات الإلكترونية بين القوى السِّياسيَّة بعد الثَّورات العربيَّة ،نوران شفيق علي، (2013)مجلة السياسة الدولية.

10- قضايا استراتيجية تحديات القوانين: الفضاء الافتراضي والقانون الدولي، الياس الصديقي (2017)

11- الإرهاب الإلكتروني: القوة في العلاقات الدولية .. نمط جديد وتحديات مختلفة ،عادل عبدالصادق (2009) مركز الدراسات السياسية والاستراتيجية، الطبعة الأولي، القاهرة.

12- القوة الإلكترونية: أسلحة الانتشار الشامل في عصر الفضاء الإلكتروني ،عادل عبدالصادق،(2012)مجلة السياسة الدولية، العدد 188.

13-كيف يمكن الاستعداد "لليوم الأسود" في الإنترنت، إيهاب خليفة (،2017) مركز المستقبل للأبحاث والدراسات.

15- الهجمات السيبرانية ،رغدة البهي (2017)،مجلة العلوم السياسية و القانون بكلية الاقتصاد و العلوم السياسة جامعة القاهرة، العدد الاول ، المركز الديمقراطي العربي.

14-تأثير تكنولوجيا الاتصال الحديثة على العلاقات الدولية ،مريم شوقي (2014)،المحور مواضيع وابحاث سياسية، الحوار المتمدن، العدد: 4338.

15- ماهية الحرب الالكترونية في ضوء قواعد القانون الدولي ،سعيد درويش، كلية الحقوق حوليات جامعة الجزائر العدد 29 الجزء الثاني.

المواقع الالكتروني

1 – علاء الدين أغا، روسيا تشن حربها السيبرانية على الغرب «ديفينس وان»، 2017، مركز البديل للتخطيط والدراسات الاستراتيجية، الرابط.el badil–pss.org // https –

2 – الموسوعة الجزائرية للدراسات السياسية الاستراتيجية ،ايهاب شوقي www.politics–dz.com2017

- https //m/hespress.com06-04-2017 **3-**

-aljazeera.net 25-03-2018**4-**

الحرب الإلكترونية ،عندما يصبح الحاسوب فتاكا، الجزيرة نت،2017/05/14، الرابط. –– aljazeera.net–**5**

6- La cyber sécurité au cœur du forum mondial des politiques de télécommunication 2013 https://news.Un.org

7-Des Forges Alix, La coopération internationale et bilatérale enjeux et rivalités ,IRESM 2013,No16,18-

http://www.siyassa.org.eg/NewsContent/2/106/3137